日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　１月２９日

出願番号
Application Number: 特願２００３－０２１０３９
[ST. 10/C]: [ＪＰ２００３－０２１０３９]

出願人
Applicant(s): キヤノン株式会社

２００４年　２月２６日

特許庁長官
Commissioner,
Japan Patent Office
今井康夫

出証番号　出証特２００４－３０１３７４８

【書類名】　特許願
【整理番号】　251538
【提出日】　平成15年 1月29日
【あて先】　特許庁長官殿
【国際特許分類】　B41K 3/00
【発明の名称】　認証装置
【請求項の数】　19
【発明者】
【住所又は居所】　東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内
【氏名】　鳥居　寛
【特許出願人】
【識別番号】　000001007
【氏名又は名称】　キヤノン株式会社
【代理人】
【識別番号】　100076428
【弁理士】
【氏名又は名称】　大塚　康徳
【電話番号】　03-5276-3241
【選任した代理人】
【識別番号】　100112508
【弁理士】
【氏名又は名称】　高柳　司郎
【電話番号】　03-5276-3241
【選任した代理人】
【識別番号】　100115071
【弁理士】
【氏名又は名称】　大塚　康弘
【電話番号】　03-5276-3241

【選任した代理人】

【識別番号】　100116894

【弁理士】

【氏名又は名称】　木村　秀二

【電話番号】　03-5276-3241

【手数料の表示】

【予納台帳番号】　003458

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0102485

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　認証装置

【特許請求の範囲】

【請求項１】　複数の認証機構を備える認証装置であって、

ユーザの認証情報を入力する入力手段と、

前記入力手段により入力された前記認証情報が前記複数の認証機構を切換え可能なユーザのものかどうかを判定する判定手段と、

前記判定手段により前記切換え可能なユーザのものと判定されると前記複数の認証機構の一覧を表示する表示制御手段と、

前記表示制御手段により表示された前記一覧の中の選択された認証機構を有効な認証機構として登録する登録手段と、

を有することを特徴とする認証装置。

【請求項２】　複数の認証機構を備える認証装置であって、

ユーザの認証情報を入力する入力手段と、

前記入力手段により入力された前記認証情報が前記複数の認証機構を切換え可能なユーザのものかどうかを判定する判定手段と、

前記判定手段により前記切換え可能なユーザのものと判定されると前記複数の認証機構の一覧を表示する表示制御手段と、

前記表示制御手段により表示された前記一覧の中の認証機構を選択する選択手段と、

前記選択手段により選択された認証機構が前記入力手段により入力された認証情報を登録している場合に、前記選択手段により選択された前記認証機構を有効な認証機構として登録する登録手段と、

を有することを特徴とする認証装置。

【請求項３】　前記入力手段は、ユーザの認証情報を記録したカードを読み取って前記認証情報を入力することを特徴とする請求項１又は２に記載の認証装置。

【請求項４】　前記入力手段は、ウェブブラウザにより前記認証情報を入力することを特徴とする請求項１又は２に記載の認証装置。

【請求項５】　前記複数の認証機構のそれぞれは、

ユーザの認証情報を登録している記憶手段と、

入力されたユーザの認証情報が前記記憶手段に登録されている場合に、当該ユーザを認証する認証判定手段と、

を有することを特徴とする請求項１乃至４のいずれか１項に記載の認証装置。

【請求項６】　前記登録手段により有効な認証機構として登録されている認証機構を起動する起動手段を更に有することを特徴とする請求項１乃至５のいずれか１項に記載の認証装置。

【請求項７】　複数の認証機構を備える認証装置における認証方法であって、

ユーザの認証情報を入力する入力工程と、

前記入力工程で入力された前記認証情報が前記複数の認証機構を切換え可能なユーザのものかどうかを判定する判定工程と、

前記判定工程で前記切換え可能なユーザのものと判定されると前記複数の認証機構の一覧を表示する表示制御工程と、

前記表示制御工程で表示された前記一覧の中の選択された認証機構を有効な認証機構として登録する登録工程と、

を有することを特徴とする認証方法。

【請求項８】　複数の認証機構を備える認証装置における認証方法であって、

ユーザの認証情報を入力する入力工程と、

前記入力工程で入力された前記認証情報が前記複数の認証機構を切換え可能なユーザのものかどうかを判定する判定工程と、

前記判定工程で前記切換え可能なユーザのものと判定されると前記複数の認証機構の一覧を表示する表示制御工程と、

前記表示制御工程で表示された前記一覧の中の認証機構を選択する選択工程と、

前記選択工程で選択された認証機構が、前記入力工程で入力された認証情報を登録している場合に前記選択工程で選択された前記認証機構を有効な認証機構と

して登録する登録工程と、
を有することを特徴とする認証方法。

【請求項９】　前記入力工程では、ユーザの認証情報を記録したカードを読み取って前記認証情報を入力することを特徴とする請求項７又は８に記載の認証方法。

【請求項１０】　前記入力工程では、ウェブブラウザにより前記認証情報を入力することを特徴とする請求項７又は８に記載の認証方法。

【請求項１１】　前記複数の認証機構のそれぞれは、ユーザの認証情報を登録する記憶ユニットを有し、入力されたユーザの認証情報が前記記憶ユニットに登録されている場合に、当該ユーザを認証する認証判定工程と、
を有することを特徴とする請求項７乃至１０のいずれか１項に記載の認証方法。

【請求項１２】　前記登録工程で有効な認証機構として登録されている認証機構を起動する起動工程を更に有することを特徴とする請求項７乃至１１のいずれか１項に記載の認証方法。

【請求項１３】　ユーザ認証情報を入力する入力工程と、
前記入力工程において入力されたユーザの認証情報を用いて第１システムに対する加入権限があるか否かを認証し、認証が成功した場合には前記ユーザを前記第１システムに加入させる第１認証工程と、
前記入力工程において入力されたユーザの認証情報を用いて第２システムに対する加入権限があるか否か認証し、認証が成功した場合には前記ユーザを前記第２システムに加入させる第２認証工程と、
前記ユーザを、前記第１システムの管理下で管理するのか、又は、前記第２システムの管理下で管理するのかを制御する制御工程と、
前記第２認証工程において前記ユーザの前記第２システムに対する認証が成功したことを確認する確認工程と、
前記第１システムから前記第２システムの管理下へユーザを移行させる命令を認識した場合には、前記制御工程は、前記確認工程において、前記ユーザが前記第２認証工程にて認証されたことを確認したことを条件として、前記第１システムにおける管理下から前記第２システムにおける管理下に前記ユーザを移行させ

るべく前記第１認証工程及び前記第２認証工程を制御することを特徴とする認証方法。

【請求項１４】　前記制御工程は、前記確認工程において、前記ユーザが前記第２認証工程にて認証されたことが確認された場合に、前記ユーザを前記第１認証工程の管理対象外となるよう前記第１認証工程を制御することを特徴とする請求項１３に記載の認証方法。

【請求項１５】　前記第１認証工程は、ユーザレベルのアクセス権限を認証するものであり、前記第２認証工程は管理者レベルのアクセス権限を管理するものであることを特徴とする請求項１３又は１４に記載の認証方法。

【請求項１６】　ユーザ認証情報を入力する入力手段と、

前記入力手段により入力されたユーザの認証情報を用いて第１システムに対する加入権限があるか否かを認証し、認証が成功した場合には前記ユーザを前記第１システムに加入させる第１認証手段と、

前記入力手段により入力されたユーザの認証情報を用いて第２システムに対する加入権限があるか否か認証し、認証が成功した場合には前記ユーザを前記第２システムに加入させる第２認証手段と、

前記ユーザを、前記第１システムの管理下で管理するのか、又は、前記第２システムの管理下で管理するのかを制御する制御手段と、

前記第２認証手段により前記ユーザの前記第２システムに対する認証が成功したことを確認する確認手段と、

前記第１システムから前記第２システムの管理下へユーザを移行させる命令を認識した場合には、前記制御手段は、前記確認手段において、前記ユーザが前記第２認証手段により認証されたことを確認したことを条件として、前記第１システムにおける管理下から前記第２システムにおける管理下に前記ユーザを移行させるべく前記第１及び第２認証手段を制御することを特徴とする認証装置。

【請求項１７】　前記制御手段は、前記確認手段により前記ユーザが前記第２認証手段により認証されたことが確認された場合に、前記ユーザを前記第１認証手段の管理対象外となるよう前記第１認証手段を制御することを特徴とする請求項１６に記載の認証装置。

【請求項１８】　前記第１認証手段は、ユーザレベルのアクセス権限を認証するものであり、前記第２認証手段は管理者レベルのアクセス権限を管理するものであることを特徴とする請求項１６又は１７に記載の認証装置。

【請求項１９】　ユーザ認証情報を入力するための入力工程と、

前記入力工程において入力されたユーザの認証情報を用いて第１システムに対する加入権限があるか否かを認証し、認証が成功した場合には前記ユーザを前記第１システムに加入させる第１認証工程と、

前記入力工程において入力されたユーザの認証情報を用いて第２システムに対する加入権限があるか否か認証し、認証が成功した場合には前記ユーザを前記第２システムに加入させる第２認証工程と、

前記ユーザを、前記第１システムの管理下で管理するのか、又は、前記第２システムの管理下で管理するのかを制御する制御工程と、

前記第２認証工程において前記ユーザの前記第２システムに対する認証が成功したことを確認する確認工程と、

前記第１システムから前記第２システムの管理下へユーザを移行させる命令を認識した場合には、前記制御工程は、前記確認工程において、前記ユーザが前記第２認証工程にて認証されたことを確認したことを条件として、前記第１システムにおける管理下から前記第２システムにおける管理下に前記ユーザを移行させるべく前記第１認証工程及び前記第２認証工程を制御することを特徴とする認証プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、複数の認証機構を備え、これら複数の認証機構の中から１つを有効にしてユーザを認証する技術に関するものである。

【０００２】

【従来の技術】

従来、ユーザが所定のユーザであるかどうかを認証し、その認証されたユーザのみがアクセスできるようにしてデータのセキュリティを高めた装置が知られて

いる。このような装置には、ユーザの認証を行う認証機構を単一だけでなく複数備えたものがある。このような複数の認証機構には、それら認証機構を階層的に配置していて、ユーザが上位の認証機構を利用する前に、より下位の認証機構により認証されるようにしたもの、或いは複数の認証機構を並列に配置し、ユーザの認証なく、それら複数の認証機構のいずれかを選択できるようにし、その選択された認証機構を用いてユーザの認証を行うものがある。

【０００３】

【発明が解決しようとする課題】

しかしながら、このような従来の技術では、それぞれ利便性とセキュリティの上で問題があった。例えば、認証機構を階層的に配置しているものは、各階層の認証機構を起動する度に、そのユーザの認証情報を提供する必要があり操作が煩わしかった。また認証機構を並列に配置しているものは、ユーザの認証なしに認証機構を切り替えられるため、操作の点では容易であるが、その分セキュリティの面で信頼性が低いという問題があった。

【０００４】

本発明は上記従来例に鑑みてなされたもので、利便性とセキュリティ上の問題を解決するために、認証機構の切り替え機能を利用するときに認証情報の提供を促すようにしたものである。

【０００５】

また本発明の目的は、認証機構を切り替えた後にユーザが適切な認証情報を持ち合わせていないがために装置を使用することができなくなることを避けるために、認証機構の切り替え前に新しい認証機構によって認証を確認することにある。

【０００６】

【課題を解決するための手段】

上記目的を達成するために本発明の認証装置は以下のような構成を備える。即ち、

複数の認証機構を備える認証装置であって、

ユーザの認証情報を入力する入力手段と、

前記入力手段により入力された前記認証情報が前記複数の認証機構を切換え可能なユーザのものかどうかを判定する判定手段と、

前記判定手段により前記切換え可能なユーザのものと判定されると前記複数の認証機構の一覧を表示する表示制御手段と、

前記表示制御手段により表示された前記一覧の中の選択された認証機構を有効な認証機構として登録する登録手段とを有することを特徴とする。

【０００７】

また上記目的を達成するために本発明の認証方法は以下のような工程を備える。即ち、

ユーザ認証情報を入力する入力工程と、

前記入力工程において入力されたユーザの認証情報を用いて第１システムに対する加入権限があるか否かを認証し、認証が成功した場合には前記ユーザを前記第１システムに加入させる第１認証工程と、

前記入力工程において入力されたユーザの認証情報を用いて第２システムに対する加入権限があるか否か認証し、認証が成功した場合には前記ユーザを前記第２システムに加入させる第２認証工程と、

前記ユーザを、前記第１システムの管理下で管理するのか、又は、前記第２システムの管理下で管理するのかを制御する制御工程と、

前記第２認証工程において前記ユーザの前記第２システムに対する認証が成功したことを確認する確認工程と、

前記第１システムから前記第２システムの管理下へユーザを移行させる命令を認識した場合には、前記制御工程は、前記確認工程において、前記ユーザが前記第２認証工程にて認証されたことを確認したことを条件として、前記第１システムにおける管理下から前記第２システムにおける管理下に前記ユーザを移行させるべく前記第１認証工程及び前記第２認証工程を制御することを特徴とする。

【０００８】

【発明の実施の形態】

以下、添付図面を参照して本発明の好適な実施の形態を詳細に説明する。尚、本実施の形態では、複数の認証機構を搭載したデータ処理装置の場合で、カード

により認証情報の提供を行う場合で説明するが、本発明はこのような構成に限定されるものではない。

【０００９】

［実施の形態１］

図１は、本発明の実施の形態に係るデータ処理装置の構成を示すブロック図である。

【００１０】

図において、１００はＣＰＵ（中央演算装置）で、本実施の形態で説明する制御方法を実行するプログラムに従って後述する処理を実行する。１０１はプログラムメモリで、ＣＰＵ１００により実行される制御プログラムが保存されている。１０２はＲＡＭで、ＣＰＵ１００による制御動作の実行時に、各種データを一時的に記憶するためのメモリエリア（ワークエリア）を提供している。１０３は表示部で、ユーザへのメッセージやメニュー、及びこの実施の形態では認証機構の一覧等を表示するのに使用される。１０４はカードリーダで、ユーザにより提示されるカードを読み取って、そのカードに記憶されている情報を読み取る。１０５は操作パネルで、キーボードやポインティングデバイス等の入力ユニットを備えており、後述する認証機構の選択等に用いられる。１１０はこれら各部とＣＰＵ１００とを接続しているシステムバスで、データバスや制御信号バス等を含んでいる。

【００１１】

尚、これ以外にも、プログラムや画像データなどを記憶している大容量の二次記憶装置（ハードディスク或いはＭＯ）、処理結果などを印刷出力するプリンタ等を備えていても良い。

【００１２】

図２は、本実施の形態１に係るデータ処理装置の機能構成を示す機能ブロック図である。尚、この実施の形態１では、これら各機能部は、ＣＰＵ１００がプログラムを実行することにより実現されている。

【００１３】

図２において、２０１は認証切り替え部で、管理者名を登録している管理者デ

ータベース２０２を管理するとともに、現在有効な認証機構を記憶している。管理者データベース２０２は、管理者の名前などの情報を保存している。２０３は認証機構起動部で、認証機構切り替え部２０１で指示された認証機構を選択して起動することができる。２０４と２０５は、この装置に搭載されている複数の認証機構の内２つを示し、それぞれ第１システムを管理する認証機構Ａと第２システムを管理する認証機構Ｂで表わされている。２０６，２０７は、ユーザの名前などの情報を保存している認証機構データベースであり、それぞれ認証機構Ａ（２０４）用のものと、認証機構Ｂ（２０５）用のものとを備えている。２０８はユーザインターフェース制御部で、操作パネル１０５よりの入力及び表示部１０３への表示を制御して、ユーザへのメッセージや警告などを表示している。カードリーダ１０４は、ユーザによりカード２０９を挿入されると、そのカード２０９に記録されているユーザの名前などの情報を読み取ることができる。この読み取ったカード情報はカードリーダ１０４から、その時点で起動されている認証機構（２０４或いは２０５）に送られる。これにより、その認証機能は対応する認証機構データベースを検索して、そのカードのユーザが、その認証機構のユーザとして登録されているかどうかを判定し、登録されている場合にそのユーザが認証される。このカード２０９はユーザが持ち歩いているものである。２１０は管理者、２１１は一般ユーザである。ここで、システムとは別個に設けられた独立したシステムも含むが、一つのシステムに複数の認証レベルに対応して認証機構が存在した場合も考えられる。例えば、第１認証レベルであるユーザレベルに対応するシステムを第１システム、第２認証レベルである管理者レベルに対応する第２認証レベルに対応するシステムを第２システムと呼ぶことにする。

【００１４】

図３は、本実施の形態に係るデータ処理装置における図２の各機能部間でのやりとりを説明する図である。

【００１５】

このデータ処理装置の起動時には、まず認証機構起動部２０３に制御が渡される。この認証機構起動部２０３は、認証機構切り替え部２０１に対して、有効な認証機構を問い合わせる（３００）。そして、その問合せに対する回答３０１に

より、認証機構Ａ（２０４）或いは認証機構Ｂ（２０５）が指示されると、認証機構起動部２０３はその指示された認証機構を起動する（３０２）。この図３では、認証機構Ａ（２０４）が有効となっており、この認証機構Ａ（２０４）が起動される場合を想定している。こうして起動された認証機構Ａ（２０４）は、ユーザインターフェース制御部２０８に対して、ユーザに対してカードリーダ１０４にカードを挿入するように指示するカード挿入指示画面を表示部１０３に表示するよう要求する（３０３）。この指示要求を受けたユーザインターフェース制御部２０８は、その要求に従ってカードの挿入を促す画面を表示部１０３に表示する。尚、ここで、カードリーダ１０４に挿入するように要求されるカードは、一般ユーザ２１１が所有している認証機構の切り替えを許されていないカードであるとする。

【００１６】

こうして、ユーザ２１１のカードがカードリーダ１０４に挿入されると（３０４）、カードリーダ制御部２２０は、そのカードから読み取った認証情報を認証機構Ａ（２０４）に渡す（３０５）。これにより認証機構Ａ（２０４）は、その認証情報を基にして認証機構Ａの認証機構データベース２０６に対して検索をかけて（３０６）、そのユーザの認証情報が認証機構Ａ（２０４）のデータベース２０６に登録されているかをみる。この検索の結果がデータベース２０６から得られて（３０７）、そのユーザ２１１の認証情報が登録されていれば、その一般ユーザ２１１が認証されたと判定する。

【００１７】

尚、ここでは認証機構Ａ（２０４）は、チャレンジ・レスポンスを利用した認証を実行することができるが、この認証形態は本発明の趣旨ではないので、ここでは詳しく説明しない。

【００１８】

図４は、図３に示す機能ブロック図における処理の流れを説明するフローチャートで、この処理を実行するプログラムはプログラムメモリ１０１に記憶されており、ＣＰＵ１００の制御の下に実行される。

【００１９】

データ処理装置が起動されるとまずステップＳ１で、認証機構切り替え部２０１に対して、有効な認証機構を問い合わせる。そしてステップＳ２に進み、有効であると指示された認証機構（ここでは認証機構Ａ（２０４））を起動する。次にステップＳ３に進み、ユーザに対してカードリーダ１０４にカードを挿入するように指示するカード挿入指示画面を表示部１０３に表示する。

【００２０】

次にステップＳ４に進み、そのユーザのカードがカードリーダ１０４に挿入されるのを待ち、カードが挿入されるとステップＳ５に進み、その挿入されたカードの情報を読み取る。そしてステップＳ６で、その読み取った認証情報を認証機構Ａ（２０４）に渡す。次にステップＳ７に進み、認証機構Ａ（２０４）は、その認証情報を基にして認証機構Ａのデータベース２０６を検索する。そしてステップＳ８で、そのユーザの認証情報が認証機構Ａ（２０４）のデータベース２０６に登録されているかを判定し、そのユーザ２１１の認証情報がデータベース２０６に登録されていれば認証成功と判断してステップＳ９に進み、その一般ユーザ２１１が認証されたと判定する。一方、ステップＳ８で、そのユーザの認証情報が認証機構Ａ（２０４）のデータベース２０６に登録されていない時は認証失敗と判断してステップＳ１０に進み、そのユーザの認証が得られないと判定する。

【００２１】

尚、ここでは認証機構Ａ（２０４）が選択された場合で説明したが、認証機構Ｂ（２０５）が選択された場合も同様にして実現可能であることはいうまでもない。

【００２２】

次に図５の機能ブロック図を参照して、ユーザにより認証機構の切換えが指示された場合を説明する。

【００２３】

図５は、本実施の形態に係るデータ処理装置において、認証機構が起動した後にユーザ（管理者）が認証機構切り替えが許されたカードを挿入する場合を説明する図である。このような認証機構切り替えが許されたカードを持つユーザを管

理者２１０と呼ぶことにする。ここでは、ユーザは予め第一の認証機構にユーザレベルで認証済みであり、カードを用いて、管理者権限の認証レベルを管理する第二の認証機構に認証機構を切り替える実施形態を示す。

【００２４】

管理者ユーザ２１０がカードをカードリーダ１０４に挿入すると（５００）、カードリーダ制御部２２０は、そのカードに記録された情報を読み取って、認証機構の切り替えが許されたカードであると判断すると、認証機構切り替え部２０１に、そのカードに記録された認証情報を渡す（５０１）。認証機構切り替え部２０１は、その渡された認証情報を基に、管理者データベース２０２に対して検索をかける（５０２）。この管理者データベース２０２に、そのカードに記録された情報が登録されている場合に認証が成功したことになる。認証が成功したことが検索結果（５０３）に基づいて判定されると、認証機構切り替え部２０２は、認証機構の選択を促す画面を表示するように、ユーザインターフェース制御部２０８に対して要求する（５０４）。この要求を渡されたユーザインターフェース制御部２０８は、このデータ処理装置に搭載された認証機構の一覧を表示部１０３に表示する。管理者ユーザ２１０が、この表示された一覧に基づいて、所望の認証機構を選択すると（５０５）、その選択された認証機構名が、ユーザインターフェース制御部２０８から認証機構切り替え部２０１に送られ（５０６）、有効な認証機構として記憶される。こうして記憶された情報は、次に、このデータ処理装置が起動されたときに認証機構起動部２０３により参照され、これに基づいて認証機構の起動が行われる。

【００２５】

図６は、図５に示す機能ブロック図における処理の流れを説明するフローチャートで、この処理を実行するプログラムはプログラムメモリ１０１に記憶されており、ＣＰＵ１００の制御の下に実行される。

【００２６】

まずステップＳ２１で、カードリーダ１０４にカードが挿入されたかどうかをみる。カードリーダ１０４にカードが挿入されるとステップＳ２２に進み、管理者ユーザ２１０が管理者用のカードをカードリーダ１０４に挿入したか、即ち、

認証機構の切り替えが許されたカードが挿入されたかどうかを判断し、そうであればステップＳ２３に進み、認証機構切り替え部２０１に、そのカードに記録された認証情報を渡して、その管理者が管理者データベース２０２に登録されている管理者であるかを判定する。そして管理者データベース２０２に、そのカードに記録された情報が登録されている場合には、認証が成功したとしてステップＳ２４に進み、認証機構の選択を促す認証機構の一覧を表示部１０３に表示する。次にステップＳ２５に進み、管理者ユーザ２１０が、この表示された一覧に基づいて、操作パネル１０５を使用して所望の認証機構を選択すると、その選択された認証機構名が有効な認証機構として記憶される。こうして記憶された情報は、次に、このデータ処理装置が起動されたときに認証機構起動部２０３により参照され、その認証機構が起動される。この間、ユーザレベルの第一の認証機構においては、ユーザは継続して認証状態であるので、認証が成功し、第二の認証機構名が有効な認証機構として記憶されるのに応答して、第一の認証機構から認証が成功したユーザを管理対象から外すと好適である。切り換え命令に応答してすぐに第一の認証機構からユーザを管理対象外とすると、第二の認証機構で認証が失敗した場合に別の管理者などがいない場合は、課題の欄で述べたように、認証機構や、システム全体を再起動したり、システムを復帰できないことにもなるからである。

【００２７】

尚、ステップＳ２２で、プログラムが管理者用のカードが挿入されたのではないと判断した場合、或いはステップＳ２３で、そのカードの持ち主が管理者として登録されていない場合は、その管理者ユーザ２１０により挿入されたカードは、認証機構の切り替えが許されたカードではないため、何もせずにそのまま処理を終了する。この間、ユーザレベルの認証機構においては、ユーザは継続して認証状態であるので、ユーザレベルの認証機構が管理するシステムに復帰できる。また場合によっては、切り換え前の認証機構の元で動作するシステムにより、「認証の切り換えが失敗した」という旨の表示を操作パネル１０５に行なってもよい。ここで、第１認証機構の管理下にあるシステムを第１システム、切り換え後の第２認証機構の管理下にあるシステムを第２システムと呼ぶ。

【００２８】

このように、カードに記憶されたユーザ名とパスワードの組や、電子証明書などをユーザ認証情報を入力する入力手段の好適な一例であるカードリータ１０４や操作パネル、カードリーダにおいて入力されたユーザの認証情報を用いて認証切り換え前の第１システムに対する加入権限があるか否かを認証し、認証が成功した場合にはユーザを前記第１システムに加入させる第１認証機構と、入力されたユーザの認証情報を用いて認証切り換え後の第２システムに対する加入権限があるか否か認証し、認証が成功した場合には前記ユーザを前記第２システムに加入させる第２認証機構と、前記ユーザを、前記第１システムの管理下で管理するのか、又は、前記第２システムの管理下で管理するのかを制御するプログラムメモリ１０１に記憶された制御プログラムと、第２認証機構において前記ユーザの前記第２システムに対する認証が成功したことを確認する確認プログラムを説明した。また、第１システムから第２システムの管理下へユーザを移行させる命令を認識した場合には、制御プログラムは、確認プログラムがユーザが第２認証機構にて認証されたことを確認したことを条件として、前記第１システムにおける管理下から前記第２システムにおける管理下に前記ユーザを移行させるべく前記第１認証機構及び前記第２認証機構を制御する。

【００２９】

以上説明したように本実施の形態１によれば、複数の認証機構を備える装置において、有効として登録されている認証機構を起動し、その起動された認証機構によりユーザを認証できる。また、その複数の認証機構の中から所望の認証機構を選択してユーザを認証するのに使用できる。

【００３０】

［実施の形態２］

本実施の形態２では、複数の認証機構を搭載したデータ処理装置において、ユーザの認証をウェブページと操作パネル１０５の両方で行う場合で説明する。

【００３１】

図７は、本発明の実施の形態２に係るデータ処理装置のハードウェア構成を示すブロック図で、前述の実施の形態１と共通する部分は同じ記号で示し、その説

明を省略する。

【００３２】

この実施の形態２に係るデータ処理装置は、通信回線７１を介して通信を行うネットワークボード７０が設けられている。

【００３３】

図８は、本実施の形態２に係るデータ処理装置の機能構成を示す機能ブロック図で、前述の実施の形態１と共通する部分は同じ記号で示している。尚、この実施の形態２においても実施の形態１と同様に、これら各機能部は、ＣＰＵ１００がプログラムを実行することにより実現されている。

【００３４】

２０２は管理者データベースで、管理者の名前などの情報を保存している。認証切り替え部２０１は、現在有効な認証機構を記憶していて、その有効な認証機構に切り換えることができる。認証機構起動部２０３は、起動すべき認証機構を判断する機構を持つ。２０４と２０５はそれぞれ、このデータ処理装置に搭載されている複数の認証機構の内２つを示し、それぞれ認証機構Ａと認証機構Ｂで示されている。２０６，２０７はそれぞれユーザの名前などの情報が保存されている認証機構データベースであり、それぞれ認証機構Ａ（２０４）用のものと、認証機構Ｂ（２０５）用のものがある。７０３は液晶パネル制御部で、操作パネル１０５と表示部１０３とを制御している。７００は認証機構切り替えウェブページ提示部で、認証機構を切り替えるためのウェブページを構築し、管理者２１０が操作する管理者ウェブブラウザ７０１にネットワーク経由で表示データを提供する。この認証機構切り替えウェブページ提示部７００は、管理者２１０を認証するためのウェブページも提供している。そのために管理者データベース２０２をも管理する。７０２は複数の認証機構で共有する認証機構ウェブページ提示部で、ユーザを認証するためのウェブページを、ユーザ２１１が操作するブラウザ７０４にネットワーク経由で提供する。管理者のウェブブラウザ７０１と、一般ユーザのウェブブラウザ７０４は、ユーザが操作するコンピュータ上で動作するウェブブラウザであり、言うまでもなくこのデータ処理装置には含まれない。

【００３５】

図９は、本実施の形態２に係るデータ処理装置の起動時におけるソフトウェアコンポーネント（図８）間のやりとりを説明する図である。

【００３６】

まず、このデータ処理装置の起動時には、認証機構起動部２０３に制御が渡される。この認証機構起動部２０３は、無条件に認証機構切り替えウェブページ提示部７００を起動する（８０１）。そして、この認証機構起動部２０３は、認証機構切り替え部２０１に有効な認証機構を問い合わせる（８０２）。その結果により（８０３）、認証機構Ａ（２０４）或いは認証機構Ｂ（２０５）を起動する（８０４）。この図８では、認証機構Ａ（２０４）が有効であるため、認証機構Ａ（２０４）を起動する場合を示している。こうして起動された認証機構Ａ（２０４）は、認証機構ウェブページ提示部７０２に認証画面を表示するよう要求する（８０５）。この要求を受けた認証機構ウェブページ提示部７０２は、ユーザの名前などの認証情報を入力するように促す画面を表示部１０３に表示する。これに応じて、一般ユーザのウェブブラウザ７０４を介して、操作パネル１０５からユーザにより認証情報が入力されると（８０６，８０７）、認証機構ウェブページ提示部７０２は、その入力された認証情報を認証機構Ａ（２０４）に渡す（８０８）。これにより認証機構Ａ（２０４）は、その入力された認証情報を基に認証機構Ａの認証機構データベース２０６に対して検索をかける（８０９）。この検索の結果（８１０）に応じて、そのユーザ２１１が認証されるかどうかが決定され、それが認証機構ウェブページ提示部７０２に通知される（８１１）。ここで、認証機構Ａ（２０４）と認証機構ウェブページ提示部７０２との間でチャレンジ・レスポンスを利用した認証を実行することができるが、この認証形態は本発明の趣旨ではないので、その説明を省略する。

【００３７】

図１０は、図９に示す機能ブロック図における処理の流れを説明するフローチャートで、この処理を実行するプログラムは図７のプログラムメモリ１０１に記憶されており、ＣＰＵ１００の制御の下に実行される。

【００３８】

この処理はデータ処理装置が起動されることにより開始され、まずステップＳ

３１で、無条件に認証機構切り替えウェブページ提示部７００を起動して認証機構切り替えウェブページを表示する。次にステップＳ３２に進み、認証機構切り替え部２０１に有効な認証機構を問い合わせる。そしてステップＳ３３で、有効な認証機構Ａ（２０４）或いは認証機構Ｂ（２０５）を起動する。こうして起動された認証機構は、ユーザの名前などの認証情報を入力するように促す画面を表示部１０３に表示する。次にステップＳ３５に進み、一般ユーザのウェブブラウザ７０４を介して、ユーザにより操作パネル１０５から認証情報が入力されるのを待ち、認証情報が入力されると、その入力された認証情報を、有効な認証機構に渡す。これにより、その認証機構は、その入力された認証情報を基に、その認証機構の認証機構データベースに対して検索をかける（ステップＳ３６）。この検索の結果、そのユーザ名等がその認証機構データベースに登録されていればステップＳ３８に進み、そのユーザが認証されたものと判定する。これに対してステップＳ３７で登録されていない場合はステップＳ３９に進み、そのユーザが認証されないと決定する。この結果は認証機構ウェブページ提示部７０２に通知されて表示される。

【００３９】

図１１は、本実施の形態２に係るデータ処理装置が起動された後に、管理者ユーザが認証機構切り替える場合を説明する図である。このような権限を持つユーザを管理者と呼ぶ。

【００４０】

まず管理者ユーザ２１０は、管理者ウェブブラウザ７０１を用いて（９０１）認証機構切り替えウェブページ提示部７００にアクセスする（９０２）。これにより、管理者ウェブブラウザ７０１には認証画面が表示される。そこで管理者ユーザ２１０は、名前などの認証情報を入力する（９０４，９０５）。こうして入力された認証情報は、認証機構切り替えウェブページ提示部７００から認証機構切り替えウェブページ提示部７００に渡される（９１０）。この渡された認証情報を基に、認証機構切り替えウェブページ提示部７００は管理者データベース２０２に対して検索をかける（９０６）。そして管理者データベース２０２に応答により（９０７）、その入力された認証情報が登録されている場合に、その管理

者の認証が成功する。こうして認証が成功すると、このデータ処理装置に搭載された認証機構の一覧が掲載されたウェブページを管理者のウェブブラウザ７０１に提示する（９０３）。これにより管理者２１０は、この一覧を参照して、所望の認証機構を選択すると（９０８）、その選択された認証機構名が認証機構切り替えウェブページ提示部７００、認証機構切り替え部２０１に渡り（９０９，９１０）、有効な認証機構として記憶される。こうして記憶された情報は、次に該装置を起動したときに認証機構起動部２０３により参照され、その有効として記憶された認証機構が起動される。

【００４１】

図１２は、図１１に示す機能ブロック図における本実施の形態２に係る処理の流れを説明するフローチャートで、この処理を実行するプログラムはプログラムメモリ１０１に記憶されており、ＣＰＵ１００の制御の下に実行される。

【００４２】

まずステップＳ４１で、管理者ユーザ２１０は、管理者ウェブブラウザ７０１を用いて認証機構切り替えウェブページ提示部７００にアクセスし、管理者ウェブブラウザ７０１に認証画面を表示する。次にステップＳ４２で、管理者ユーザ２１０により名前などの認証情報が入力されるとステップＳ４３に進み、入力された認証情報が、管理者データベース２０２に登録されているか否かを認証機構切り替えウェブページ提示部７００により検索し、登録されていればステップＳ４４に進み、このデータ処理装置に搭載された認証機構の一覧が掲載されたウェブページを管理者のウェブブラウザ７０１に提示する。これにより表示部１０３にその一覧が表示される。そしてステップＳ４５に進み、管理者２１０がこの一覧を参照して、所望の認証機構を選択するとステップＳ４６に進み、その選択された認証機構名が認証機構切り替えウェブページ提示部７００、認証機構切り替え部２０１に渡り（９０９，９１０）、有効な認証機構として登録される。こうして記憶された情報は、次に該装置を起動したときに認証機構起動部２０３により参照され、その有効として記憶された認証機構が起動される。

【００４３】

一方、ステップＳ４３で、その入力された認証情報が管理者として登録されて

いない時はステップＳ４７に進み、その管理者の認証情報が登録されていない旨を表示部１０３に表示する。尚、このステップＳ４７の処理は例えば前述の図６のステップＳ２２，ステップＳ２３で「Ｎｏ」の場合に実行されても良い。

【００４４】

以上説明したように本実施の形態２によれば、複数の認証機構を備える装置において、有効として登録されている認証機構を起動し、その起動された認証機構のウェブページにユーザのウェブブラウザによりアクセスしてユーザを認証できる。

【００４５】

また、ウェブブラウザにより認証切り替えウェブページにアクセスして、複数の認証機構の中から所望の認証機構を選択してユーザを認証するのに使用できる。

【００４６】

［実施の形態３］

次に本発明の実施の形態３に係るデータ処理装置について説明する。

【００４７】

図１３は、本実施の形態３に係るデータ処理装置の機能構成を示す機能ブロック図で、前述の実施の形態と共通する部分は同じ記号で示している。尚、この実施の形態３に係るデータ処理装置のハードウェア構成は前述の実施の形態１と同様であるため、その説明を省略する。この実施の形態３の特徴は、ユーザの認証をユーザインターフェース制御部２０８のより制御される操作パネル１０５からの入力により行うことを特徴としている。

【００４８】

認証切り替え部２０１は、現在有効な認証機構を記憶している。認証機構起動部２０３は、この認証切り替え部２０１よりの有効な認証機構を示す情報に基づいて、有効とされている認証機構を起動する。２０４と２０５は、このデータ処理装置に搭載されている複数の認証機構の内２つを示し、それぞれ認証機構Ａと認証機構Ｂで示す。２０６と２０７は、各認証機構毎にユーザの名前などの情報を保存している認証機構データベースであり、それぞれ認証機構Ａ（２０４）用

のものと、認証機構Ｂ（２０５）用のものを含む。２０８は、複数の認証機構で共有するユーザインターフェース制御部で、このデータ処理装置の操作パネル１０５と表示部１０３とを制御する。

【００４９】

図１４は、本実施の形態３に係るデータ処理装置における図１３で示したソフトウェアコンポーネント間のやりとりを示した図である。

【００５０】

まずこのデータ処理装置の起動時に、認証機構起動部２０３に制御が渡されると、この認証機構起動部２０３は、認証機構切り替え部２０１に有効な認証機構を問い合わせる（１３００）。その結果（１３０１）により、認証機構Ａ（２０４）又は認証機構Ｂ（２０５）を起動する。この図１４では、認証機構Ａ（２０４）が有効な認証機構として起動される場合を示している。こうして起動された認証機構Ａ（２０４）は、ユーザインターフェース制御部２０８に認証画面を表示するよう要求する（１３０４）。この要求を受けたユーザインターフェース制御部２０８は、ユーザの名前などの認証情報を入力するように促す画面を表示部１０３に表示する。この表示に基づいて、ユーザ２１１により操作パネル１０５を使用して認証情報が入力されると（１３０５）、ユーザインターフェース制御部２０８は、その操作パネル１０５から入力された認証情報を認証機構Ａ（２０４）に渡す（１３０６）。これにより認証機構Ａ（２０４）は、その認証情報を基に、認証機構Ａの認証機構データベース２０６に対して、ユーザ２１１の認証情報が登録されているかを調べる（１３０７）。その結果（１３０８）に応じて、ユーザ２１１が認証されるかどうかが決定され、その結果がユーザインターフェース制御部２０８に送られて表示される（１３０９）。

【００５１】

図１５は、図１４に示す実施の形態３に係る機能ブロック図における処理の流れを説明するフローチャートで、この処理を実行するプログラムはプログラムメモリ１０１に記憶されており、ＣＰＵ１００の制御の下に実行される。

【００５２】

この処理はデータ処理装置が起動されることにより開始され、まずステップＳ

５１で、有効な認証機構を判定して、有効として記憶されている認証機構Ａ（２０４）又は認証機構Ｂ（２０５）を起動する。こうして認証機構が起動されるとステップＳ５２に進み、ユーザインターフェース制御部２０８により認証画面を表示部１０３に表示する。次にステップＳ５３では、この表示に基づいて、操作パネル１０５を使用して、ユーザ２１１により認証情報が入力されるのを待ち、認証情報が入力されるとステップＳ５４に進み、その入力された認証情報を、その認証機構に渡す。これによりステップＳ５５で、その認証機構は、その入力された認証情報を基に、その認証機構の認証機構データベースに、その入力されたユーザ２１１の認証情報が登録されているか検索する。登録されている時はステップＳ５６に進み、そのユーザ２１１が認証されたと判定する。一方、ステップＳ５５で登録されていない時はステップＳ５７に進み、そのユーザが認証ができなかったと判断する。

【００５３】

図１６は、本実施の形態３において、認証機構が起動した後にユーザ（管理者）が認証機構を切り替える場合のソフトウェアコンポーネント間のやりとりを表す図である。このような権限を持つユーザを管理者と呼ぶことにする。

【００５４】

管理者ユーザ２１０が、前述と同様な手順で管理者として認証された後のやりとりを説明する。管理者ユーザ２１０が管理者として認証された後、管理者ユーザ２１０は、操作パネル１０５によりユーザインターフェース制御部２０８を用いて、適当な方法で認証機構選択画面を表示部１０３に表示させる。このような機能の実装はメニューシステムなどを使えば自明なので省略する。こうして認証機構の選択画面が表示される。この選択画面には、このデータ処理装置に搭載されている認証機構の一覧が表示される。管理者２１０は、この表示された一覧に基づいて、操作パネル１０５から所望の認証機構を選択すると（１５００）、ユーザインターフェース制御部２０８は、管理者２１０に名前などの認証情報の入力を促す画面を表示する。これにより管理者２１０が、操作パネル１０５から認証情報を入力すると（１５０１）、ユーザインターフェース制御部２０８は、その選択された認証機構に認証情報の検証を依頼する（１５０２）。ここでは認証

機構Ｂ（２０５）が選ばれたものとする。認証機構Ｂ（２０５）は、受け取った認証情報を基に、認証機構Ｂデータベース２０７に検索をかける（１５０３）。これにより認証機構Ｂデータベース２０７は、その検索結果を認証機構Ｂ（２０５）に返す（１５０４）。そして、その結果が認証成功を表していた場合、選ばれた認証機構名が認証機構切り替え部２０１に送られ（１５０５，１５０６）、有効な認証機構として記憶される。こうして記憶された情報は、次にこのデータ処理装置を起動したときに認証機構起動部２０３で参照される。

【００５５】

図１７は、本実施の形態３に係るデータ処理装置が起動された後に、管理者ユーザが認証機構を切り替える場合を説明する図である。このような権限を持つユーザを管理者と呼ぶ。

【００５６】

この処理は認証機構の切り替えが指示されるとことにより開始され、まずステップＳ６１で、管理者ユーザ２１０が認証情報を入力すると、前述と同様にして管理者データベース２０２に、その認証情報が登録されているか否かに応じて、管理者として登録されているか否かを判定する（ステップＳ６２）。管理者として登録されていない時はステップＳ６９に進み、登録された管理者ではないため認証機構の切換えができない旨を表示してこの処理を終了する。

【００５７】

ステップＳ６２で、管理者ユーザ２１０が管理者として認証されるとステップＳ６３に進み、管理者ユーザ２１０は、ユーザインターフェース制御部２０８を用いて、適当な方法で認証機構の選択画面を表示させる。これにより、このデータ処理装置に搭載されている認証機構の一覧が表示される。次にステップＳ６４に進み、管理者２１０は、この表示された一覧に基づいて、操作パネル１０５を使用して所望の認証機構が選択されるとステップＳ６５に進み、その選択された認証機構を選択する。次にステップＳ６６に進み、管理者ユーザ２１０に名前などの認証情報の入力を催促する画面を表示する。これにより管理者２１０が、その認証情報を操作パネル１０５により入力するとステップＳ６７に進み、その選択された認証機構に認証情報の検証を依頼する。ここでは、その認証機構は、そ

の受け取った認証情報を基に、認証機構データベースを検索し、そのデータベースにその管理者の認証情報が登録されているかを判別する。その結果、登録されていると判断されるとステップＳ６８に進み、その選ばれた認証機構名を認証機構切り替え部２０１に送って有効な認証機構として登録する。こうして記憶された情報は、次にこのデータ処理装置を起動したときに認証機構起動部２０３で参照される。

【００５８】

以上説明したように本実施の形態３によれば、複数の認証機構を備える装置において、有効として登録されている認証機構を起動し、操作パネルを使用して入力されたユーザの認証情報に基づいて、その認証機構によりユーザを認証できる。また、管理者は操作パネルを用いて、複数の認証機構の中から所望の認証機構を選択してユーザを認証するのに使用できる。

【００５９】

尚、前述したデータ処理装置の具体例としては、複写機としての機能以外に、例えばファクシミリやプリンタ等の機能を備えた多機能複写機が挙げられる。この複写機では、一般ユーザは、その時点で選択されている認証機構（実質的にはソフトウェアで構成され、場合によってはカードリーダ等の特定のハードウェアを使用する）を使用して認証された場合にのみ、その複写機を使用してコピーやファクシミリ送信等を行うことができる。もちろん認証不可能なユーザは、この複写機を使用することができない。

【００６０】

又、管理者として登録されているユーザは、必要に応じて認証機構を切り換えることができる。こうして認証機構が切り替えられると、例えばウェブページを使用してユーザの認証が可能になったり、また各ユーザが認証のために入力する情報も変更されることになる。これにより一般のユーザの中でも、この複写機を使用可能なユーザが変更されることになる。またこのような認証機構の切り換えにより、この多機能複写機の、例えば基本設定を変更する権限が与えられているユーザと、それ以外のユーザとの区別を付けることもできる。

【００６１】

［その他の実施の形態］

なお本発明は、複数の機器(例えばホストコンピュータ、インターフェース機器、リーダ、プリンタなど)から構成されるシステムに適用しても、一つの機器からなる装置(例えば、複写機、ファクシミリ装置など)に適用しても良い。又、例えば、スキャナ機能、プリント機能、コピー機能、ファクシミリ機能、プリンタ機能、ネットワーク機能等の複数の機能のうちの、何れか１つの機能のみを有する単一機能の装置においても本発明は適用可能であるし、上記複数の機能のうちの、例えばコピー機能とプリンタ機能の２つの機能を有するデジタル複合機やコピー／ファクシミリ／プリンタ等の３つの機能或いは３つ以上の機能を有すデジタル複合機等の、上記複数の機能のうちの２つ以上の機能を少なくとも有する複合装置においても本発明は適用可能である。

【００６２】

また、本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはＣＰＵまたはＭＰＵ）が記憶媒体に格納されたプログラムコードを読み出し実行することによっても達成されることは言うまでもない。

【００６３】

この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。

【００６４】

プログラムコードを供給するための記憶媒体としては、例えば、フロッピィディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、磁気テープ、不揮発性のメモリカード、ＲＯＭなどを用いることが出来る。

また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼動しているＯＳ（オペレーティングシステム）などが実際の処理の一部を行い、その処理によって前述した実施形態の機能が実現さ

れる場合も含まれることは言うまでもない。

【００６５】

さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部または全部を行い、その処理によって前述した実施の形態の機能が実現される場合も含まれることは言うまでもない。

【００６６】

以上説明したように本実施の形態によれば、複数の認証機構を備える装置において、認証機構切り替え時に切り替えようとするユーザの認証を行うことができる。また、並列に構成された認証機構を切り替える場合にも、その切り替えを指示したユーザの認証を行うようにしているのので、認証機構を切り替えた後に認証情報データベースが変わってしまったために装置を利用できなくなる状況を防ぐことができる。

【００６７】

【発明の効果】

以上説明したように本発明によれば、利便性とセキュリティ上の問題を解決することができる。

【００６８】

また本発明によれば、認証機構を切り替えた後にユーザが適切な認証情報を持ち合わせていないがために装置を使用することができなくなることを避けるために、認証機構の切り替え前に新しい認証機構によって認証を確認することができる。

【図面の簡単な説明】

【図１】

本発明の実施の形態に係るデータ処理装置のハードウェア構成を説明するブロック図である。

【図２】

実施の形態１に係るデータ処理装置の機能構成を説明する機能ブロック図である。

【図３】

実施の形態１に係るデータ処理装置において、カードによりユーザの認証を行う場合を説明する機能ブロック図である。

【図４】

実施の形態１に係るデータ処理装置において、カードによりユーザの認証を行う場合の処理を説明するフローチャートである。

【図５】

実施の形態１に係るデータ処理装置において、管理者により認証機構を切り換える場合を説明する機能ブロック図である。

【図６】

実施の形態１に係るデータ処理装置において、管理者により認証機構を切り換える場合の処理を説明するフローチャートである。

【図７】

本発明の実施の形態２に係るデータ処理装置のハードウェア構成を説明するブロック図である。

【図８】

実施の形態２に係るデータ処理装置の機能構成を説明する機能ブロック図である。

【図９】

実施の形態２に係るデータ処理装置において、ユーザのウェブブラウザを用いてユーザの認証を行う場合を説明する機能ブロック図である。

【図１０】

実施の形態２に係るデータ処理装置において、ユーザのウェブブラウザを用いてユーザの認証を行う処理を説明するフローチャートである。

【図１１】

実施の形態２に係るデータ処理装置において、管理者のウェブブラウザを用いて認証機構の切り替えを行う場合を説明する機能ブロック図である。

【図１２】

実施の形態２に係るデータ処理装置において、管理者のウェブブラウザを用いて認証機構の切り替えを行う処理を説明するフローチャートである。

【図１３】

本発明の実施の形態３に係るデータ処理装置の機能構成を説明する機能ブロック図である。

【図１４】

本実施の形態３に係るデータ処理装置において、ユーザインターフェースを用いてユーザの認証を行う場合を説明する機能ブロック図である。

【図１５】

本実施の形態３に係るデータ処理装置において、ユーザインターフェースを用いてユーザの認証を行う処理を説明するフローチャートである。

【図１６】

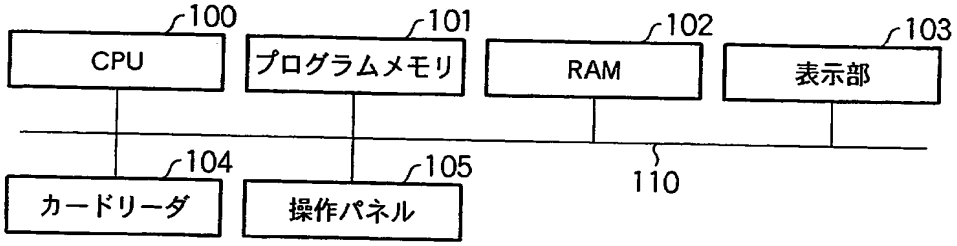
実施の形態３に係るデータ処理装置において、管理者がユーザインターフェースを用いて認証機構の切り替えを行う場合を説明する機能ブロック図である。

【図１７】

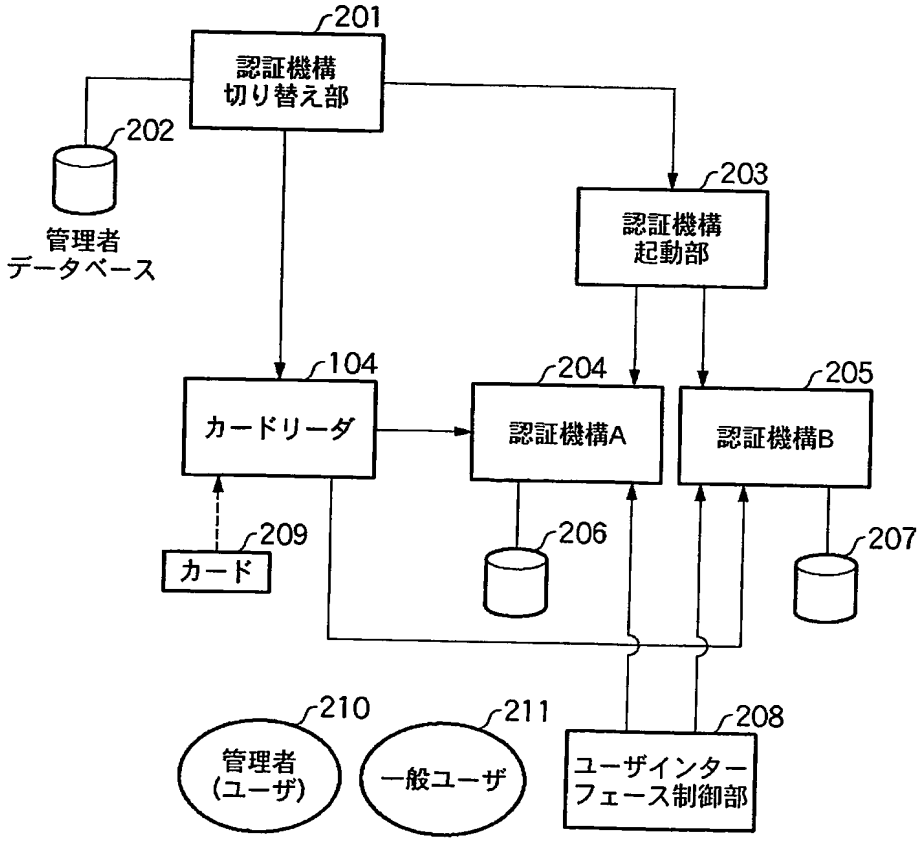
実施の形態３に係るデータ処理装置において、管理者がユーザインターフェースを用いて認証機構の切り替えを行う処理を説明するフローチャートである。

【書類名】　図面

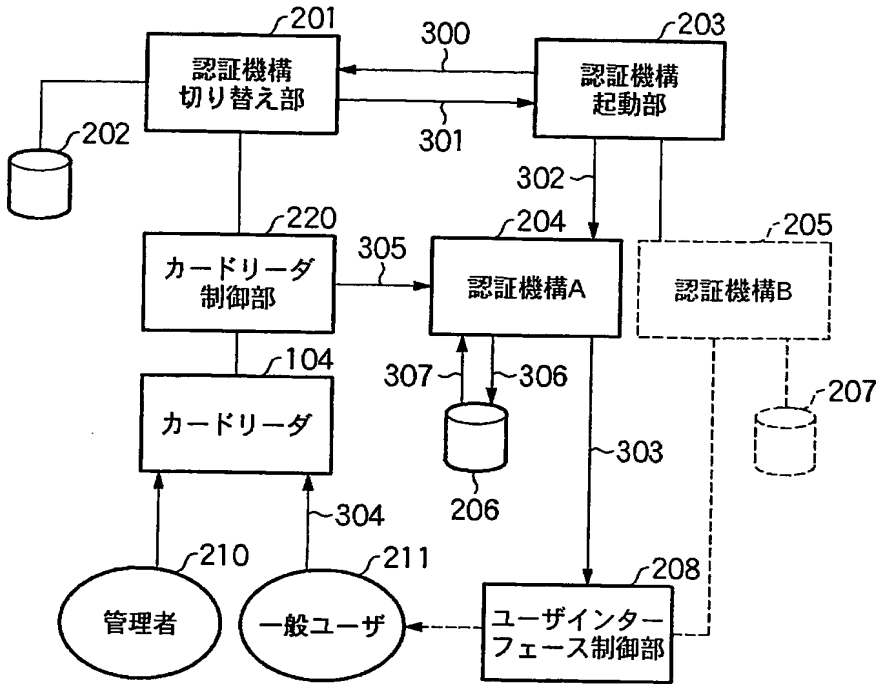
【図１】


100
CPU
101
プログラムメモリ
102
RAM
103
表示部
110
104
カードリーダ
105
操作パネル

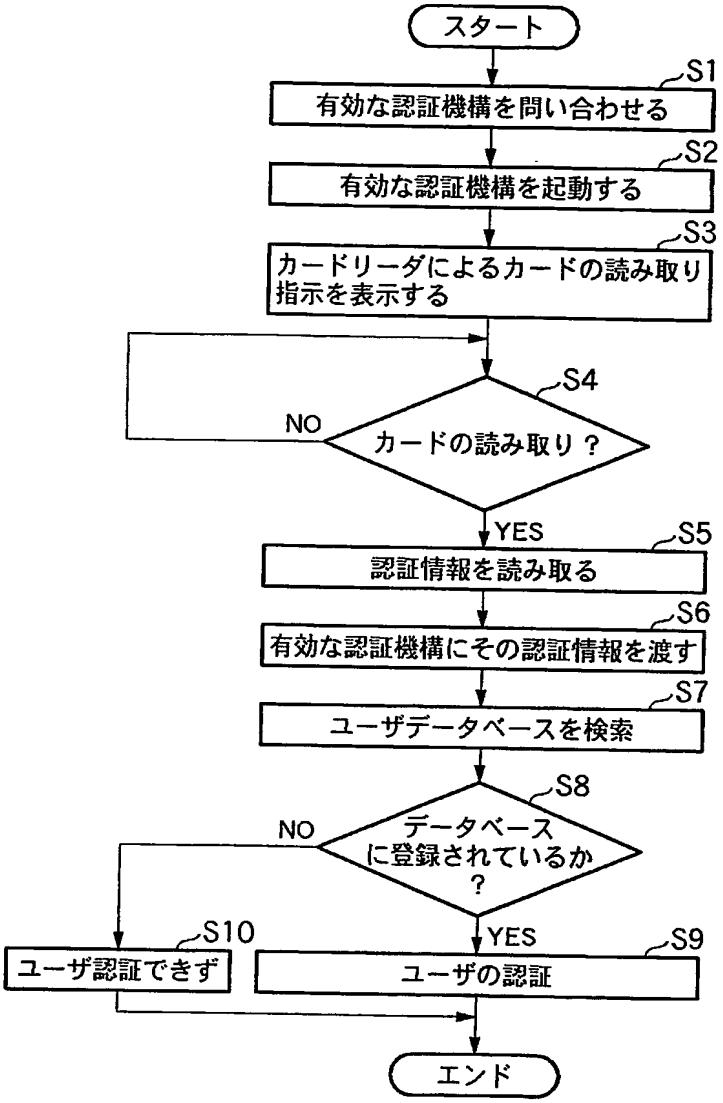
【図２】


201
認証機構
切り替え部
202
管理者
データベース
203
認証機構
起動部
104
カードリーダ
204
認証機構A
205
認証機構B
209
カード
206
207
210
管理者
(ユーザ)
211
一般ユーザ
208
ユーザインター
フェース制御部

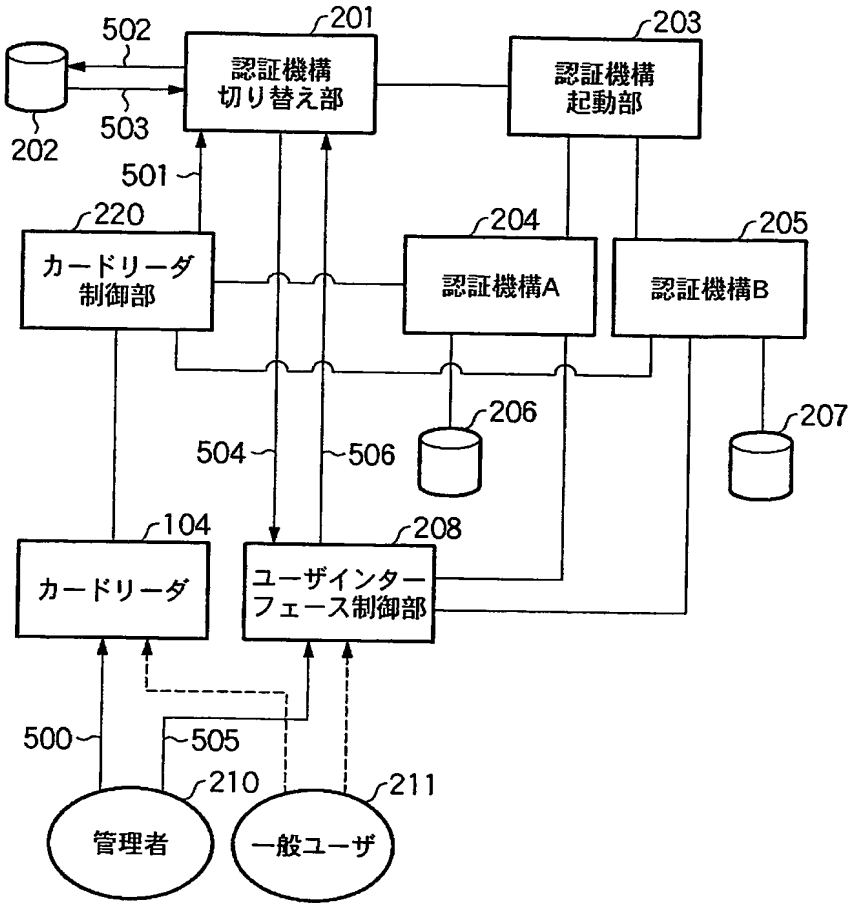
【図３】


201
認証機構
切り替え部
300
301
203
認証機構
起動部
202
302
220
カードリーダ
制御部
305
204
認証機構A
205
認証機構B
104
カードリーダ
307
306
207
303
206
304
210
211
208
管理者
一般ユーザ
ユーザインター
フェース制御部

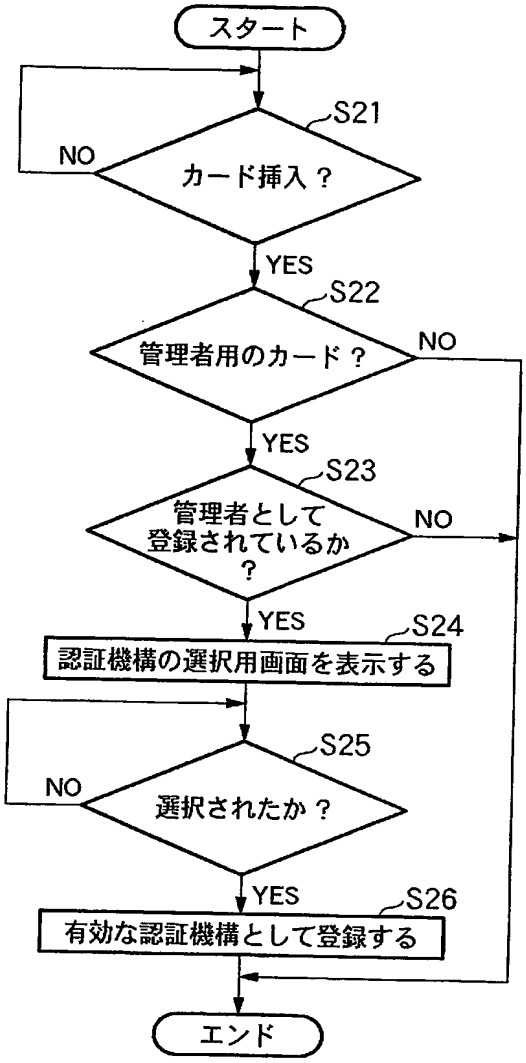
【図４】


スタート
S1
有効な認証機構を問い合わせる
S2
有効な認証機構を起動する
S3
カードリーダによるカードの読み取り指示を表示する
S4
NO
カードの読み取り？
YES
S5
認証情報を読み取る
S6
有効な認証機構にその認証情報を渡す
S7
ユーザデータベースを検索
S8
NO
データベースに登録されているか？
YES
S9
ユーザの認証
S10
ユーザ認証できず
エンド

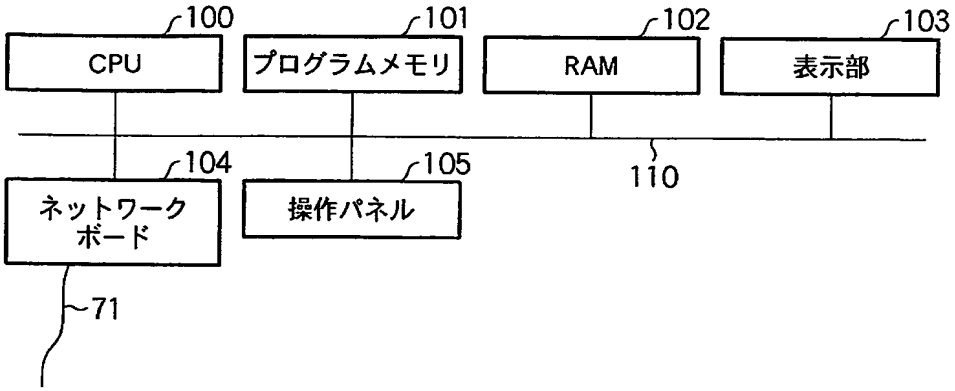
【図５】


502
201
203
認証機構
切り替え部
認証機構
起動部
202
503
501
220
204
205
カードリーダ
制御部
認証機構A
認証機構B
206
207
504
506
104
208
カードリーダ
ユーザインター
フェース制御部
500
505
210
211
管理者
一般ユーザ

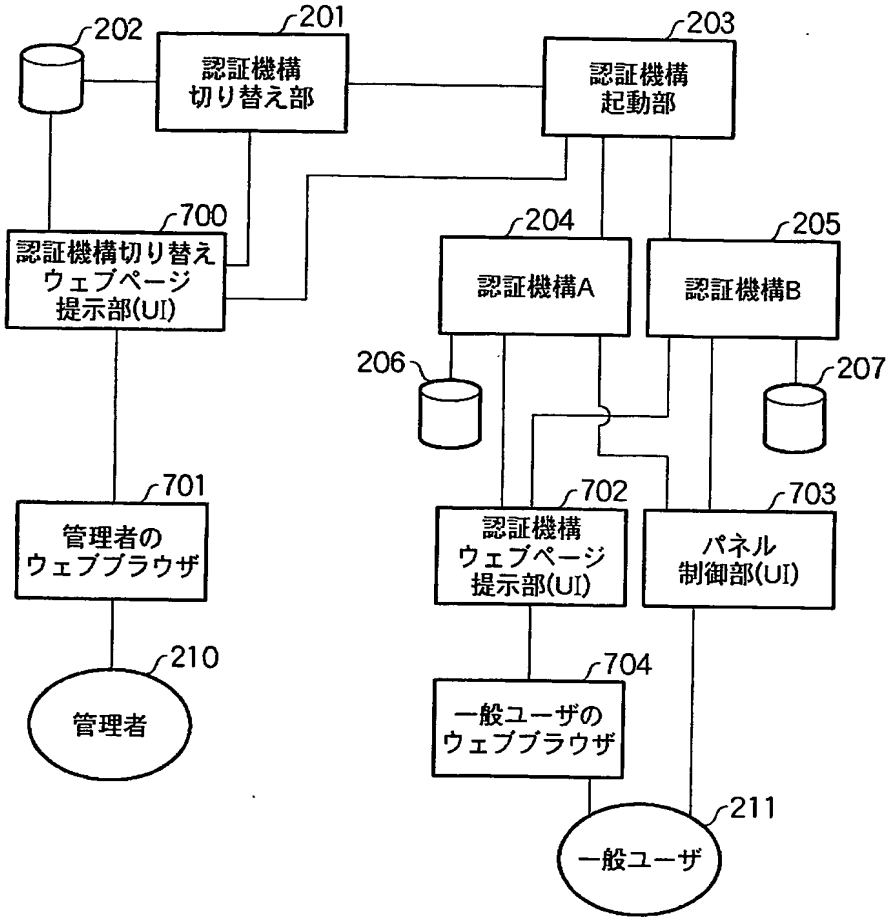
【図６】


スタート
S21
NO
カード挿入？
YES
S22
管理者用のカード？
NO
YES
S23
管理者として
登録されているか
？
NO
YES
S24
認証機構の選択用画面を表示する
S25
NO
選択されたか？
YES
S26
有効な認証機構として登録する
エンド

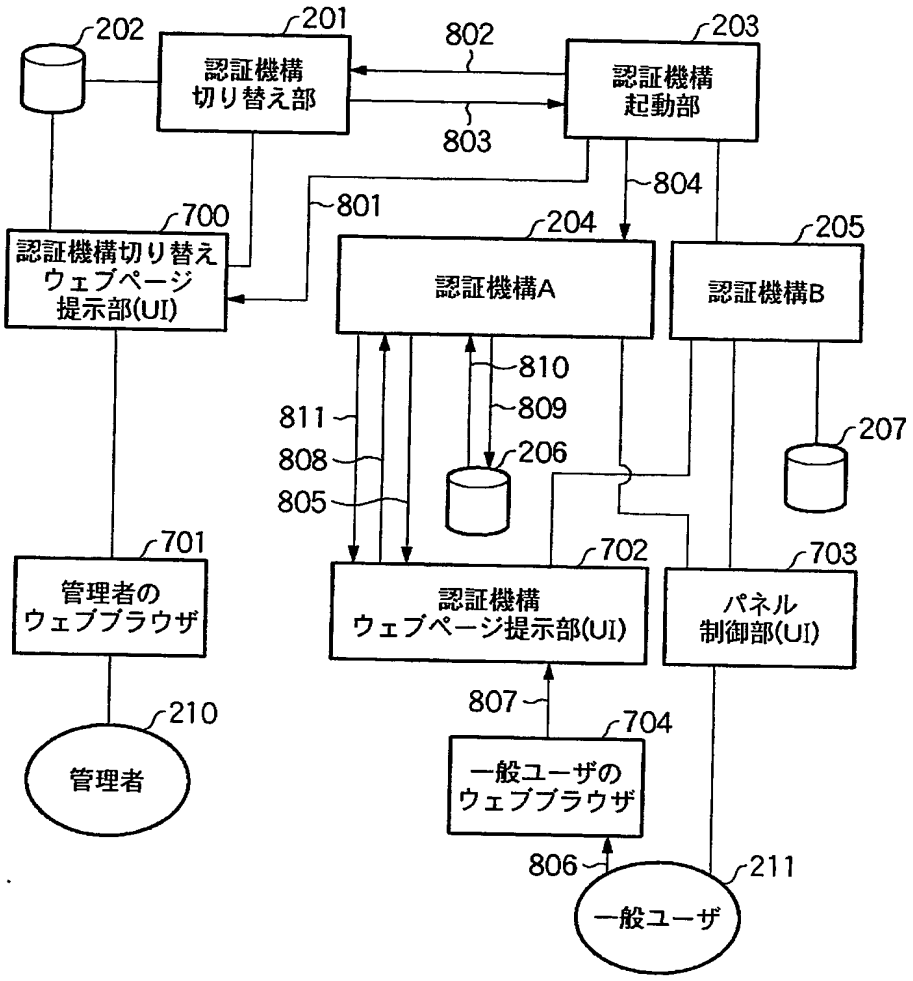
【図７】


100
CPU
101
プログラムメモリ
102
RAM
103
表示部
110
104
ネットワーク
ボード
105
操作パネル
71

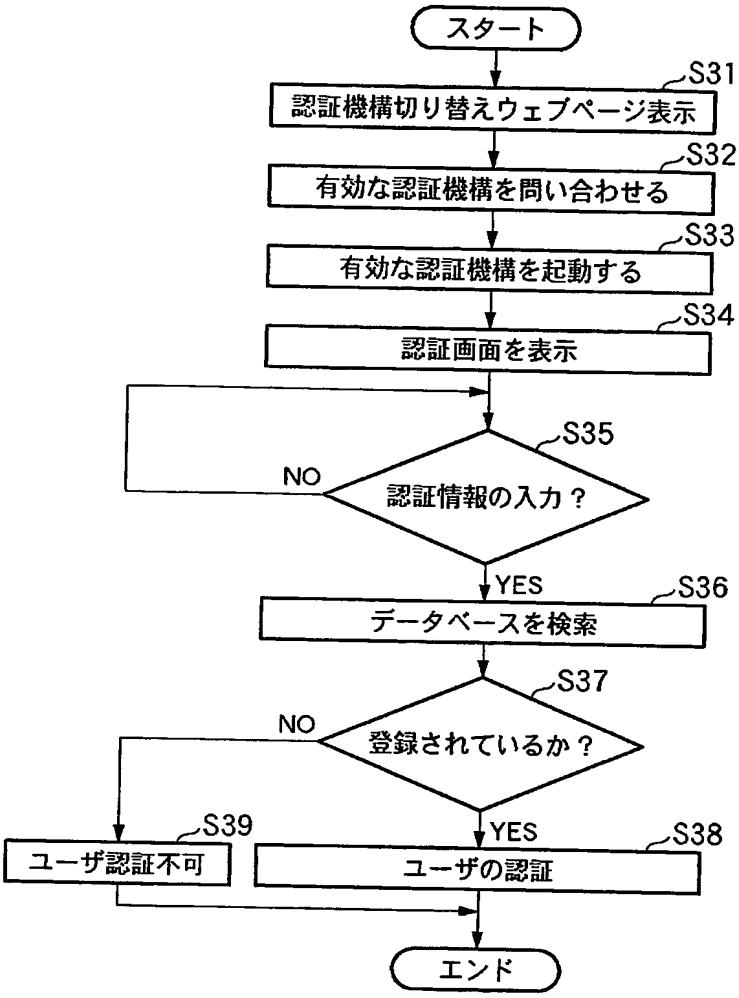
【図８】


202
201
認証機構
切り替え部
203
認証機構
起動部
700
認証機構切り替え
ウェブページ
提示部(UI)
204
認証機構A
205
認証機構B
206
207
701
管理者の
ウェブブラウザ
702
認証機構
ウェブページ
提示部(UI)
703
パネル
制御部(UI)
210
管理者
704
一般ユーザの
ウェブブラウザ
211
一般ユーザ

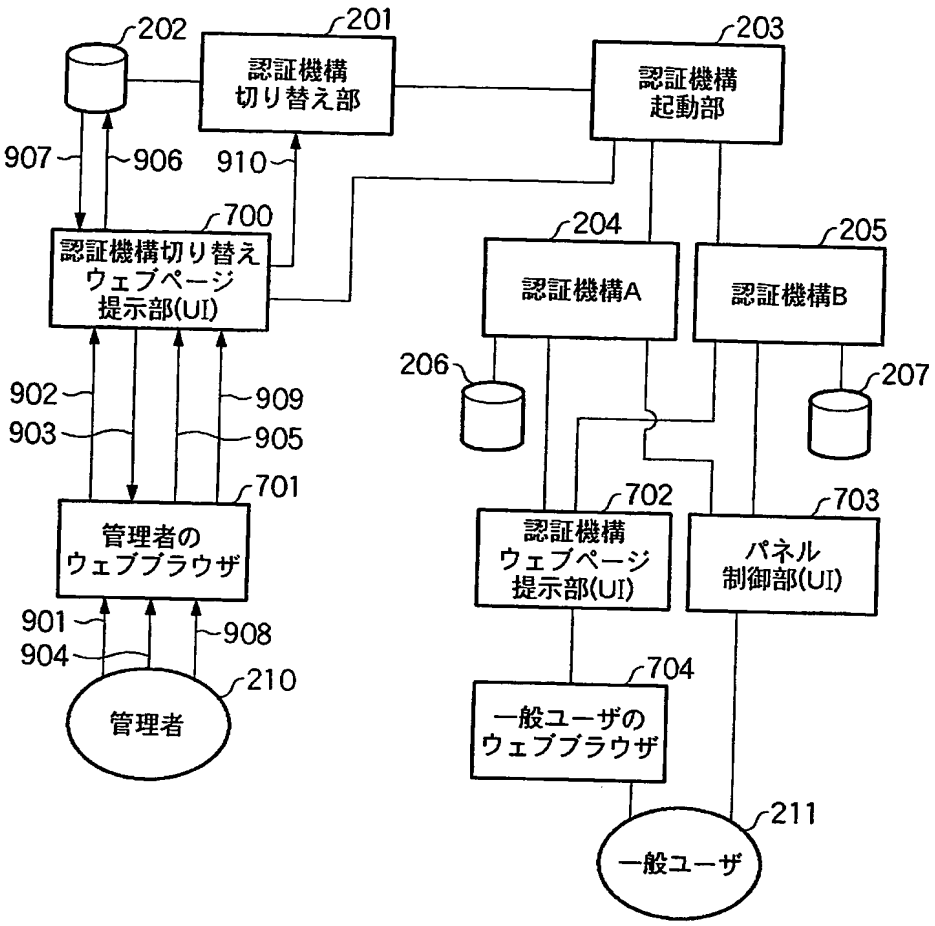
【図９】


202
201
認証機構
切り替え部
802
803
203
認証機構
起動部
804
801
700
認証機構切り替え
ウェブページ
提示部(UI)
204
認証機構A
205
認証機構B
810
809
811
808
805
206
207
701
管理者の
ウェブブラウザ
702
認証機構
ウェブページ提示部(UI)
703
パネル
制御部(UI)
807
704
一般ユーザの
ウェブブラウザ
210
管理者
806
211
一般ユーザ

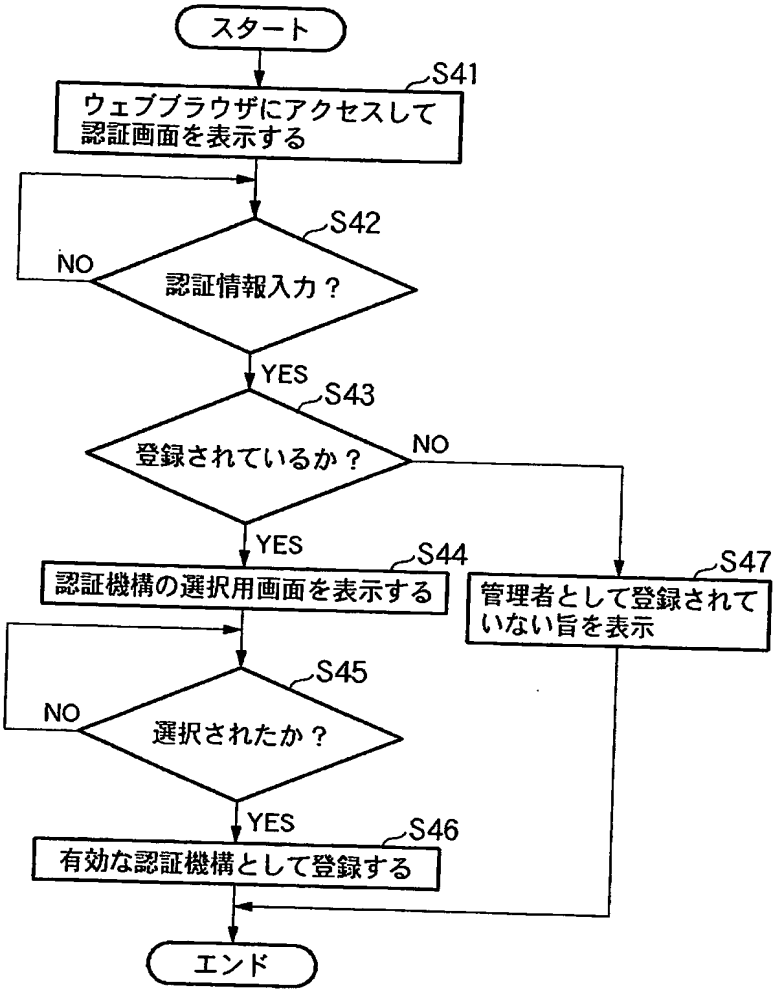
【図１０】


スタート
S31
認証機構切り替えウェブページ表示
S32
有効な認証機構を問い合わせる
S33
有効な認証機構を起動する
S34
認証画面を表示
S35
NO
認証情報の入力？
YES
S36
データベースを検索
S37
NO
登録されているか？
YES
S39
ユーザ認証不可
S38
ユーザの認証
エンド

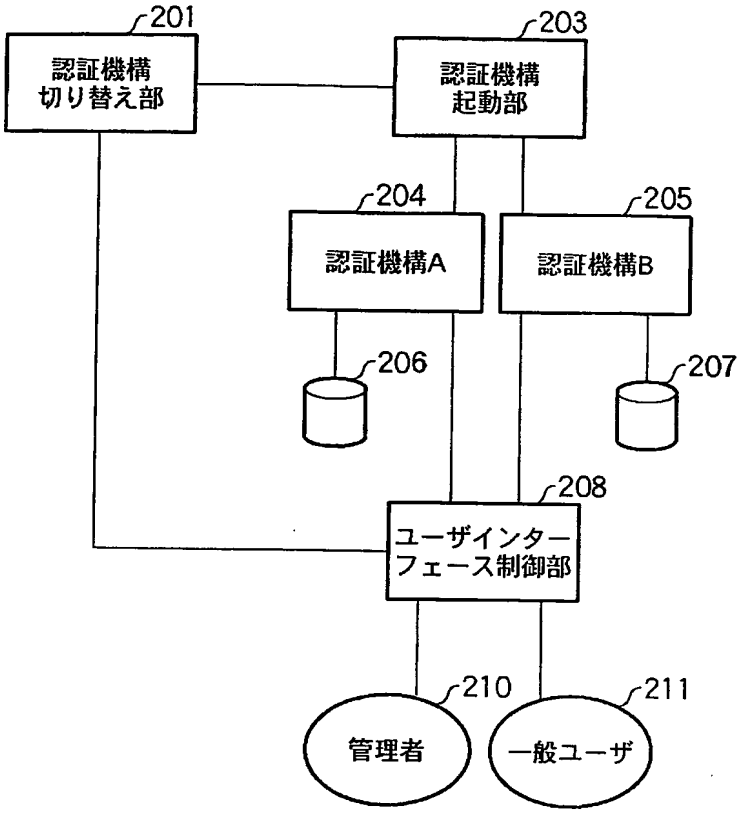
【図１１】


202
201
認証機構
切り替え部
203
認証機構
起動部
907
906
910
700
認証機構切り替え
ウェブページ
提示部(UI)
204
認証機構A
205
認証機構B
206
207
902
903
909
905
701
管理者の
ウェブブラウザ
702
認証機構
ウェブページ
提示部(UI)
703
パネル
制御部(UI)
901
904
908
210
管理者
704
一般ユーザの
ウェブブラウザ
211
一般ユーザ

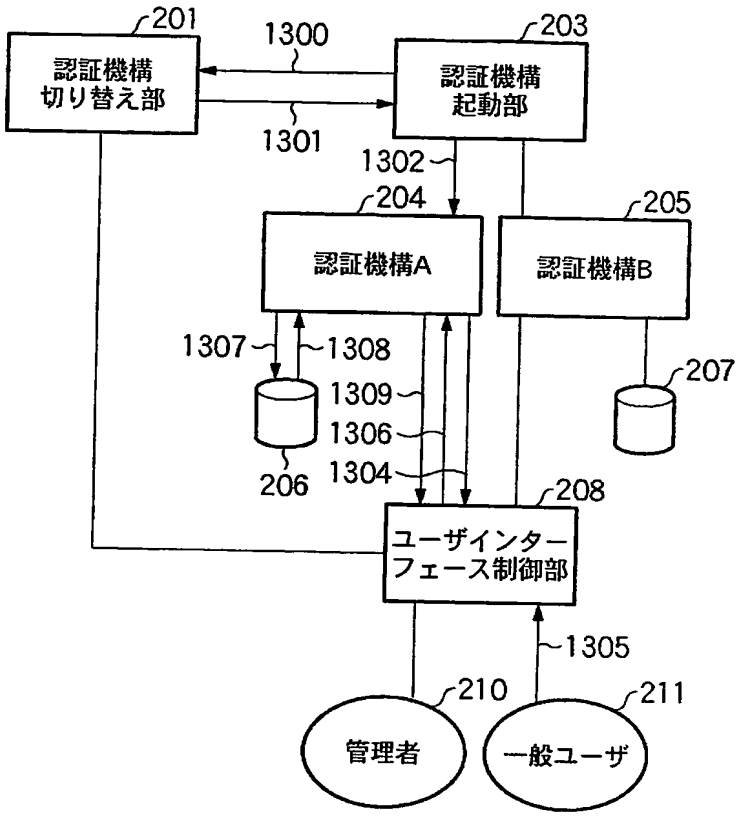
【図１２】


スタート
S41
ウェブブラウザにアクセスして
認証画面を表示する
S42
NO
認証情報入力？
YES
S43
登録されているか？
NO
YES
S44
認証機構の選択用画面を表示する
S47
管理者として登録されて
いない旨を表示
S45
NO
選択されたか？
YES
S46
有効な認証機構として登録する
エンド

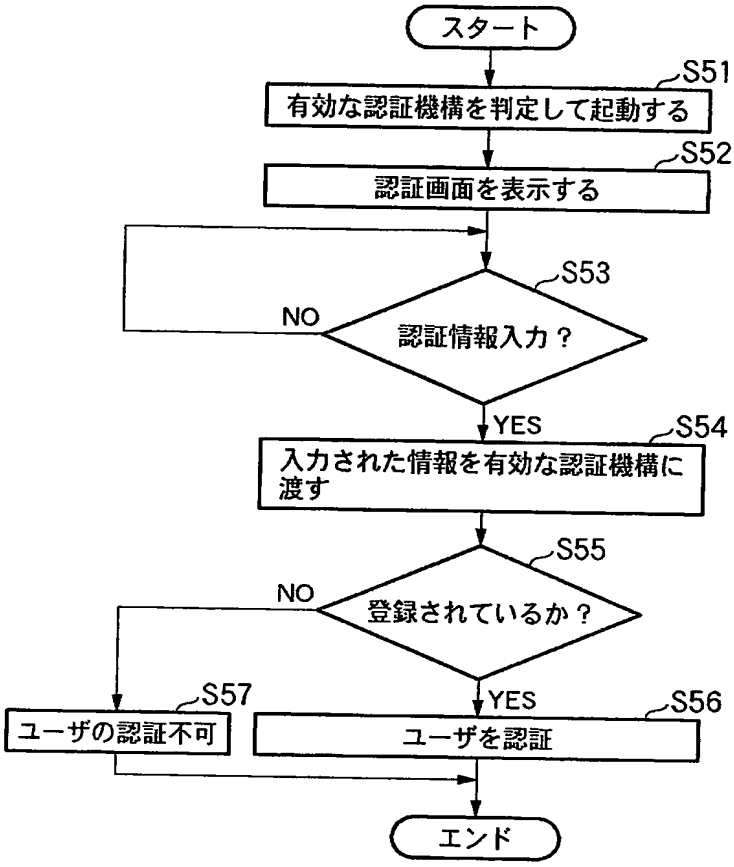
【図１３】


201
認証機構
切り替え部
203
認証機構
起動部
204
認証機構A
205
認証機構B
206
207
208
ユーザインター
フェース制御部
210
管理者
211
一般ユーザ

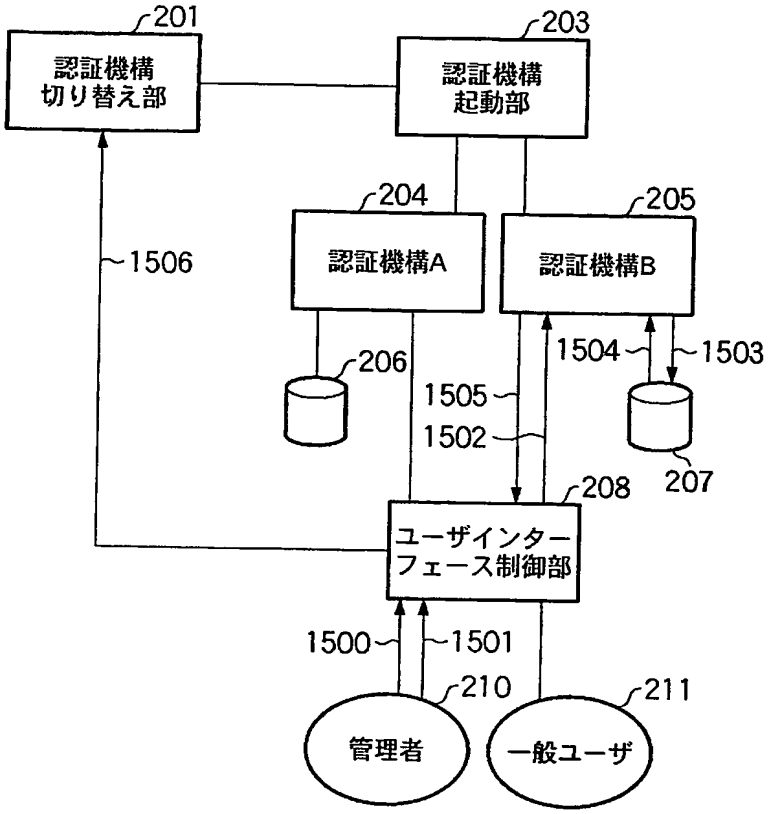
【図１４】


201
認証機構
切り替え部
1300
1301
203
認証機構
起動部
1302
204
認証機構A
205
認証機構B
1307
1308
1309
1306
1304
206
207
208
ユーザインター
フェース制御部
1305
210
管理者
211
一般ユーザ

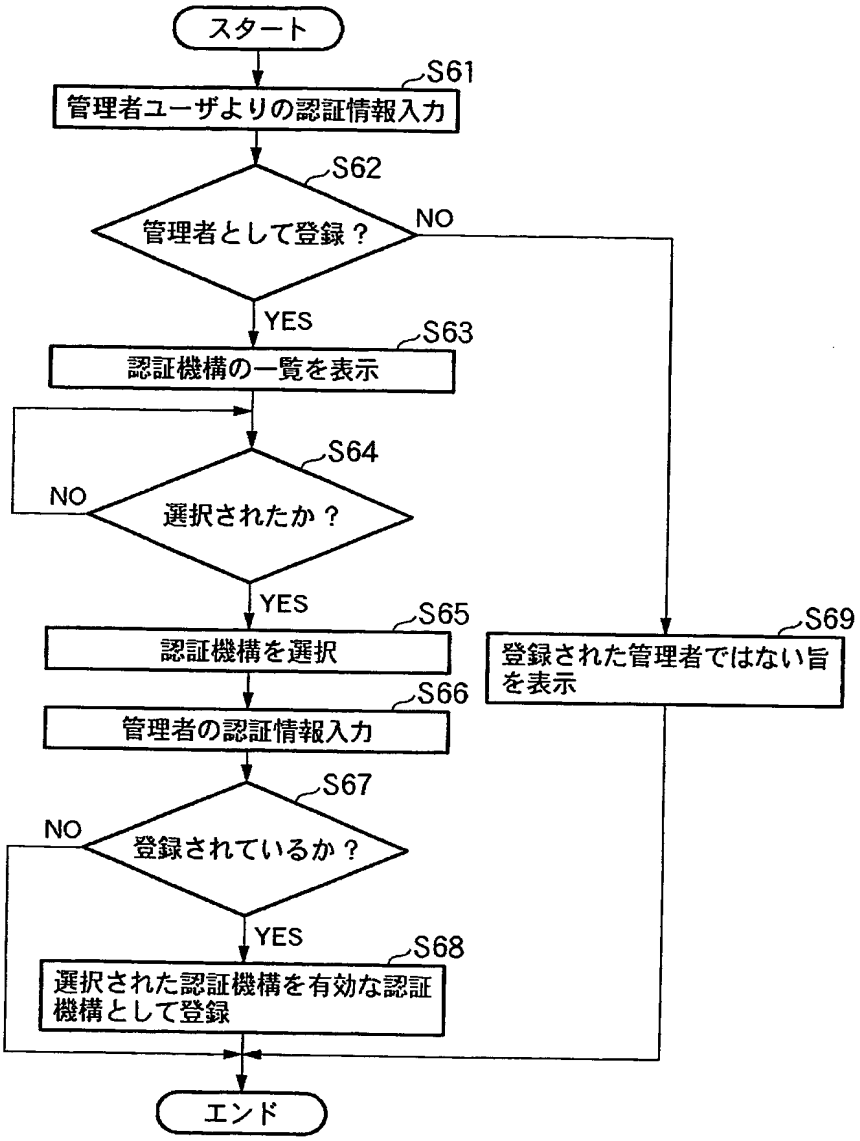
【図１５】


スタート
S51
有効な認証機構を判定して起動する
S52
認証画面を表示する
S53
NO
認証情報入力？
YES
S54
入力された情報を有効な認証機構に渡す
S55
NO
登録されているか？
YES
S56
ユーザを認証
S57
ユーザの認証不可
エンド

【図１６】


201
認証機構
切り替え部
203
認証機構
起動部
204
認証機構A
205
認証機構B
1506
206
1505
1502
1504
1503
207
208
ユーザインター
フェース制御部
1500
1501
210
211
管理者
一般ユーザ

【図１７】


スタート
S61
管理者ユーザよりの認証情報入力
S62
管理者として登録？
NO
YES
S63
認証機構の一覧を表示
S64
NO
選択されたか？
YES
S65
認証機構を選択
S66
管理者の認証情報入力
S67
NO
登録されているか？
YES
S68
選択された認証機構を有効な認証機構として登録
S69
登録された管理者ではない旨を表示
エンド

【書類名】　要約書

【要約】

【課題】　利便性とセキュリティ上の問題を解決する。

【解決手段】　複数の認証機構を備える認証装置であって、ユーザの認証情報を入力するカードリーダにより入力された認証情報が複数の認証機構を切換え可能なユーザのものかどうかを判定し（Ｓ２３）、切換え可能なユーザのものと判定されると複数の認証機構の一覧を表示し（２４）、その表示された一覧の中の選択された認証機構を有効な認証機構として登録する（Ｓ２６）。

【選択図】　図６

特願２００３－０２１０３９

出　願　人　履　歴　情　報

識別番号　　[０００００１００７]

１．変更年月日　　１９９０年　８月３０日
[変更理由]　　新規登録
住　所　　東京都大田区下丸子３丁目３０番２号
氏　名　　キヤノン株式会社

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- [x] BLACK BORDERS
- [ ] IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- [x] FADED TEXT OR DRAWING
- [ ] BLURRED OR ILLEGIBLE TEXT OR DRAWING
- [ ] SKEWED/SLANTED IMAGES
- [ ] COLOR OR BLACK AND WHITE PHOTOGRAPHS
- [ ] GRAY SCALE DOCUMENTS
- [ ] LINES OR MARKS ON ORIGINAL DOCUMENT
- [x] REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- [ ] OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.